2025/2447

2025.12.5.

A BIZOTTSÁG (EU) 2025/2447 VÉGREHAJTÁSI RENDELETE

(2025. december 4.)

az (EU) 2018/1727 európai parlamenti és tanácsi rendeletnek az információk biztonságos kezelésére és közlésére szolgáló decentralizált informatikai rendszer létrehozására és használatára vonatkozó műszaki előírások, intézkedések és egyéb követelmények tekintetében történő alkalmazására vonatkozó szabályok megállapításáról

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel az Európai Unió Büntető Igazságügyi Együttműködési Ügynökségéről (Eurojust) és a 2002/187/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről szóló, 2018. november 14-i (EU) 2018/1727 európai parlamenti és tanácsi rendeletre ([1]) és különösen annak 22a. cikke (3) bekezdésére, valamint 22b. cikke (1) bekezdésének a), b), c) és d) pontjára,

mivel:

(1) Az (EU) 2018/1727 rendelet meghatározza az Eurojust új digitális belső infrastruktúrájának keretét, valamint rendelkezik a tagállamok illetékes nemzeti hatóságai és az Eurojust közötti decentralizált biztonságos digitális kommunikációs rendszer létrehozásáról.

(2) A biztonságos digitális kommunikációt a decentralizált informatikai rendszeren keresztül kell folytatni. A decentralizált informatikai rendszer létrehozásához meg kell határozni a kommunikációs módszereket és kommunikációs protokollokat, az információbiztonsági minimumszabályokat biztosító technikai intézkedéseket, valamint az említett rendszer megvalósítására vonatkozó biztonsági és minimális rendelkezésre állási célkitűzéseket.

(3) Az (EU) 2018/1727 rendelet 22a. cikkének (1) bekezdése szerint a decentralizált informatikai rendszernek a tagállamok és az Eurojust informatikai rendszereiből, valamint az interoperábilis e-CODEX hozzáférési pontokból kell állnia, amelyeken keresztül ezek az informatikai rendszerek összekapcsolódnak. A decentralizált informatikai rendszer e rendeletben meghatározott műszaki előírásainak és egyéb követelményeinek figyelembe kell venniük ezt a keretet.

(4) A decentralizált informatikai rendszer hozzáférési pontjainak az (EU) 2022/850 európai parlamenti és tanácsi rendelet ([2]) 3. cikkének (3) bekezdésében meghatározott engedélyezett e-CODEX hozzáférési pontokon kell alapulniuk.

(5) A decentralizált informatikai rendszert egy nagyobb, e-CODEX-alapú decentralizált informatikai rendszer, az úgynevezett igazságügyi digitális adatcsererendszer (JUDEX) keretében valósítják meg. Ezért biztosítani kell a horizontális fejlesztésekkel kapcsolatos hatékony információcserét.

(6) Az (EU) 2018/1727 rendelet 22a. cikkének (4) bekezdésével összhangban a tagállamok és az Eurojust azt is választhatják, hogy nemzeti informatikai rendszerük helyett a Bizottság által kifejlesztett referenciaimplementáció-szoftvert alkalmazzák háttérrendszerként. Az interoperabilitás biztosítása érdekében mind a nemzeti informatikai rendszereknek, mind a referenciaimplementáció-szoftvernek ugyanazokat a műszaki előírásokat és követelményeket kell teljesíteniük.

(7) A terrorista bűncselekményekre és a súlyos szervezett bűnözésre vonatkozó adatokat strukturált módon kell továbbítani az adatok minőségének és relevanciájának javítása, valamint annak biztosítása érdekében, hogy az adatokat hatékonyabban lehessen integrálni az Eurojust ügyviteli rendszerébe, és jobban össze lehessen vetni az abban már tárolt adatokkal. A terrorista bűncselekményekkel kapcsolatos büntetőeljárás alá vont személyek azonosítása céljából az Eurojustnak továbbítható ujjnyomatadatok és fényképek esetében meg kell határozni a formátumot és a továbbításra vonatkozó technikai előírásokat.

([1]) HL L 295., 2018.11.21., 138. o., ELI: http://data.europa.eu/eli/reg/2018/1727/oj.

([2]) Az Európai Parlament és a Tanács (EU) 2022/850 rendelete (2022. május 30.) a polgári és büntetőügyekben folytatott igazságügyi együttműködés területén történő, határokon átnyúló elektronikus adatcserére szolgáló számítógépes rendszerről (e-CODEX-rendszer) és az (EU) 2018/1726 rendelet módosításáról (HL L 150., 2022.6.1., 1. o., ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(8) Az Eurojust megkönnyíti és támogatja az igazságügyi együttműködésre irányuló megkeresések kiadását és végrehajtását, ideértve a kölcsönös elismerés elvét érvényesítő eszközökön alapuló megkereséseket és határozatokat. Az illetékes nemzeti hatóságok számára lehetővé kell tenni, hogy a decentralizált informatikai rendszeren keresztül kérjék az Eurojust segítségét és koordinációját.

(9) A hatékonyság és a következetesség biztosítása érdekében fontos, hogy az (EU) 2018/1727 rendelet alapján megállapítandó műszaki előírások összeegyeztethetők legyenek az (EU) 2023/2844 ([3]), az (EU) 2023/1543 ([4]) és az (EU) 2024/3011 ([5]) európai parlamenti és tanácsi rendeletben meghatározott műszaki előírásokkal, valamint az Eurojustnak az illetékes nemzeti hatóságok támogatására vonatkozó megbízatása szempontjából releváns jövőbeli digitalizációs intézkedésekkel.

(10) A decentralizált informatikai rendszeren keresztül lehetővé kell tenni továbbá az Eurojust és az illetékes nemzeti hatóságok közötti bármely egyéb kommunikációt, például az információkezelés eredményeire vonatkozó információk nyújtását, ideértve az (EU) 2018/1727 rendelet 22. cikkével összhangban az ügyviteli rendszerben már tárolt ügyekkel való kapcsolat fennállását, amennyiben az Eurojust hivatalból jár el, vagy az említett rendelet 4. cikke (1) bekezdésének j) pontja szerint a népirtással, az emberiesség elleni bűncselekményekkel, a háborús bűncselekményekkel és a kapcsolódó bűncselekményekkel kapcsolatos bizonyítékok megőrzése, elemzése és tárolása céljából az Eurojustnak továbbított információkat.

(11) Annak biztosítása érdekében, hogy e rendelet figyelembe vegye az Eurojust operatív igényeit, az (EU) 2018/1727 rendelet 22a. cikkének (3) bekezdésével összhangban konzultációra került sor az Eurojusttal.

(12) Az Európai Unióról szóló szerződéshez és az Európai Unió működéséről szóló szerződéshez csatolt, az Egyesült Királyságnak és Írországnak a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség tekintetében fennálló helyzetéről szóló 21. jegyzőkönyv 4. cikkével összhangban Írország a 2019. szeptember 9-én kelt levelében értesítést nyújtott be azon szándékáról, hogy elfogadja és magára nézve kötelezőnek tekinti az (EU) 2018/1727 rendeletet. Az (EU) 2019/2006 bizottsági határozat ([6]) megerősítette ezt a részvételt. Az (EU) 2023/2131 európai parlamenti és tanácsi rendelet ([7]), amely módosította az (EU) 2018/1727 rendeletet annak érdekében, hogy lehetővé tegye az Eurojust és az illetékes nemzeti hatóságok közötti biztonságos digitális kommunikációs csatornák létrehozását, egyúttal megteremtette e rendelet jogalapját. Mivel Írország nem jelentette be, hogy részt kíván venni az (EU) 2023/2131 rendelet elfogadásában és alkalmazásában, és nem nyújtott be értesítést azon szándékáról, hogy elfogadja és magára nézve kötelezőnek tekinti az említett rendeletet, a 21. jegyzőkönyv 1. és 2. cikkével és 4a. cikkének (1) bekezdésével összhangban az (EU) 2023/2131 rendelet Írországra nézve nem kötelező és nem alkalmazandó. Ezért Írország nem vesz rész ennek a rendeletnek az elfogadásában.

(13) Az Európai Unióról szóló szerződéshez és az Európai Unió működéséről szóló szerződéshez csatolt, Dánia helyzetéről szóló 22. jegyzőkönyv 1. és 2. cikke értelmében Dánia nem vett részt az (EU) 2018/1727 rendelet elfogadásában. Ezért ez a rendelet Dániára nézve nem kötelező és nem alkalmazandó.

([3]) Az Európai Parlament és a Tanács (EU) 2023/2844 rendelete (2023. december 13.) a határokon átnyúló polgári, kereskedelmi és büntetőügyekben folytatott igazságügyi együttműködés és az igazságszolgáltatáshoz való hozzáférés digitalizációjáról, valamint az igazságügyi együttműködés területén egyes jogi aktusok módosításáról (HL L, 2023/2844, 2023.12.27., ELI: http://data.europa.eu/eli/reg/2023/2844/oj).

([4]) Az Európai Parlament és a Tanács (EU) 2023/1543 rendelete (2023. július 12.) a büntetőeljárás során az elektronikus bizonyítékokkal kapcsolatban, valamint a büntetőeljárást követően a szabadságvesztés-büntetések végrehajtása céljából kibocsátott, közlésre kötelező európai határozatokról és megőrzésre kötelező európai határozatokról (HL L 191., 2023.7.28., 118. o., ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

([5]) Az Európai Parlament és a Tanács (EU) 2024/3011 rendelete (2024. november 27.) a büntetőeljárás átadásáról (HL L 2024/3011, 2024.12.18., ELI: http://data.europa.eu/eli/reg/2024/3011/oj).

([6]) A Bizottság (EU) 2019/2006 határozata (2019. november 29.) Írországnak az Európai Unió Büntető Igazságügyi Együttműködési Ügynökségéről (Eurojust) szóló (EU) 2018/1727 európai parlamenti és tanácsi rendeletben való részvételéről (HL L 310., 2019.12.2., 59. o., ELI: http://data.europa.eu/eli/dec/2019/2006/oj).

([7]) Az Európai Parlament és a Tanács (EU) 2023/2131 rendelete (2023. október 4.) az (EU) 2018/1727 európai parlamenti és tanácsi rendeletnek és a 2005/671/IB tanácsi határozatnak a terrorizmussal kapcsolatos ügyekben folytatott digitális információcsere tekintetében történő módosításáról (HL L, 2023/2131, 2023.10.11., ELI: http://data.europa.eu/eli/reg/2023/2131/oj).

(14) Az (EU) 2018/1725 európai parlamenti és tanácsi rendelet ([8]) 42. cikkének (1) bekezdésével összhangban a Bizottság egyeztetett az európai adatvédelmi biztossal, aki 2025. október 21-én véleményt nyilvánított.

(15) Az e rendeletben előírt intézkedések összhangban vannak az (EU) 2018/1727 rendelet 22c. cikkével létrehozott bizottság véleményével,

ELFOGADTA EZT A RENDELETET:

1. cikk

A decentralizált informatikai rendszerre vonatkozó műszaki előírások

Az (EU) 2018/1727 rendelet 22b. cikke (1) bekezdésének a), b), c) és d) pontjában említett decentralizált informatikai rendszerre vonatkozó műszaki előírásokat, intézkedéseket és célkitűzéseket e rendelet I. melléklete határozza meg.

2. cikk

Digitális eljárási szabványok

Az (EU) 2018/1727 rendelet 22a. cikkének (3) bekezdésében említett decentralizált informatikai rendszeren keresztül történő elektronikus kommunikációra alkalmazandó digitális eljárási szabványokat e rendelet II. melléklete határozza meg.

3. cikk

Az ujjlenyomatok és fényképek továbbítására vonatkozó műszaki előírások

Az ujjnyomatoknak és fényképeknek az (EU) 2018/1727 rendelet 22a. cikkének (3) bekezdésében említett továbbítására vonatkozó technikai előírásokat és azok formátumát e rendelet III. melléklete határozza meg.

4. cikk

Hatálybalépés

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Ez a rendelet a Szerződéseknek megfelelően teljes egészében kötelező és közvetlenül alkalmazandó a tagállamokban.

Kelt Brüsszelben, 2025. december 4-én.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN

([8]) Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (HL L 295., 2018.11.21., 39. o., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

I. MELLÉKLET

A DECENTRALIZÁLT INFORMATIKAI RENDSZERRE VONATKOZÓ MŰSZAKI ELŐÍRÁSOK, INTÉZKEDÉSEK ÉS CÉLOK

1. **Bevezetés és alkalmazási kör**

Ez a melléklet az (EU) 2018/1727 rendelet szerinti információcserét szolgáló decentralizált informatikai rendszerre vonatkozó műszaki előírásokat, intézkedéseket és célokat rögzíti.

Az informatikai rendszer decentralizált jellege lehetővé teszi az illetékes nemzeti hatóságok és az Eurojust közötti közvetlen és biztonságos adatcserét.

2. **Fogalommeghatározások**

E melléklet alkalmazásában:

2.1. „Hypertext Transfer Protocol Secure" vagy „HTTPS": titkosított kommunikációs és biztonságos kapcsolódási csatornák;

2.2. „eredet letagadhatatlansága": azon intézkedések, amelyek igazolják az adatok integritását és eredetét olyan módszerek segítségével, mint a digitális tanúsítás, a nyilvános kulcsú infrastruktúra, az elektronikus aláírások és az elektronikus bélyegzők;

2.3. „beérkezés letagadhatatlansága": azon intézkedések, amelyek igazolják a kibocsátó számára az adatok meghatározott címzetthez történő beérkezését olyan módszerek segítségével, mint a digitális tanúsítás, a nyilvános kulcsú infrastruktúra, az elektronikus aláírások és az elektronikus bélyegzők;

2.4. „SOAP (egyszerű objektumelérési protokoll)": a World Wide Web Konzorcium szabványainak megfelelő olyan üzenetküldő protokollra vonatkozó előírás, amely a webes szolgáltatások számítógépes hálózatokon belüli megvalósítására vonatkozó strukturált információ cseréjéhez alkalmazandó;

2.5. „REST (Representational State Transfer)": a hálózatba kapcsolt alkalmazások tervezésére szolgáló architektúrastílus, amely állapotfüggetlen kliens-szerver kommunikációs modellre támaszkodik, és szabványos módszerekkel végez műveleteket a jellemzően strukturált formátumú erőforrásokon;

2.6. „webszolgáltatás": olyan szoftverrendszer, amelynek célja az együttműködő gépek közötti kapcsolat támogatása egy adott hálózaton belül, és amely géppel feldolgozható formátumban leírt interfésszel rendelkezik;

2.7. „adatcsere": üzenetek és iratok cseréje a decentralizált informatikai rendszeren keresztül;

2.8. „e-CODEX": az (EU) 2022/850 rendelet 3. cikkének (1) bekezdésében meghatározott e-CODEX-rendszer;

2.9. „uniós e-igazságügyi alapszókészlet": az (EU) 2022/850 rendelet mellékletének 4. pontjában meghatározott uniós e-igazságügyi alapszókészlet;

2.10. „ebMS": az OASIS keretrendszerben kidolgozott ebXML üzenetküldő szolgáltatás, amely lehetővé teszi az elektronikus üzleti dokumentumok SOAP protokollon keresztül történő biztonságos, megbízható és interoperábilis cseréjét. Támogatja a vállalkozások közötti integrációt a különböző rendszerekben;

2.11. „AS4": alkalmazhatósági nyilatkozat 4, az ebMS 3.0 profilját képező OASIS szabvány, amely leegyszerűsíti a vállalkozások közötti biztonságos és interoperábilis üzenetküldést olyan nyílt szabványok alkalmazásával, mint a SOAP és a WS-Securtiy;

2.12. „helyreállítási időre vonatkozó célkitűzés”: biztonsági eseményt követően a szolgáltatás helyreállításának maximális elfogadható ideje;

2.13. „helyreállítási pontra vonatkozó célkitűzés”: az adatvesztés maximális elfogadható mennyisége meghibásodás esetén.

3. **Az elektronikus eszközök útján történő kommunikáció módjai**

3.1. A decentralizált informatikai rendszer szolgáltatásalapú kommunikációs megoldásokat, például webszolgáltatásokat vagy más újrahasználható komponenseket és szoftvermegoldásokat alkalmaz az üzenetek és iratok cseréje céljából.

3.2. Ez konkrétan az (EU) 2022/850 rendelet 5. cikkének (2) bekezdésében meghatározott e-CODEX hozzáférési pontokon keresztüli kommunikációt jelenti. Ezért a hatékony és interoperábilis, határokon átnyúló adatcsere biztosítása érdekében a decentralizált informatikai rendszernek támogatnia kell az e-CODEX-rendszeren keresztüli kommunikációt.

4. **Kommunikációs protokollok**

4.1. A decentralizált informatikai rendszer biztonságos internetes protokollokat használ a következőkhöz:

a) kommunikáció az illetékes hatóságok és az Eurojust között a decentralizált informatikai rendszeren belül;

b) kommunikáció a 7.1. pontban említett illetékes hatósági/bírósági adatbázissal.

4.2. A strukturált adatok és metaadatok meghatározása és továbbítása tekintetében a decentralizált informatikai rendszer komponensei átfogó és széles körben elfogadott ágazati szabványokon és protokollokon (például SOAP, REST) alapulnak.

4.3. Az átviteli és üzenetküldési protokollok tekintetében a decentralizált informatikai rendszer biztonságos szabványalapú protokollokon alapul, például:

a) a határokon átnyúló adatcseréhez AS4 profil, amely titkosítás és letagadhatatlanság mellett biztosítja a biztonságos és megbízható üzenetküldést;

b) a JSON és XML formátumokat támogató kommunikációhoz HTTPS/RESTful API-k;

c) a nagy megbízhatóságú interakciókhoz SOAP, ezen belül a hitelesítéshez és a titkosításhoz WS-Security.

4.4. A zökkenőmentes és interoperábilis adatcsere érdekében a decentralizált informatikai rendszer által használt kommunikációs protokoll megfelel a vonatkozó interoperabilitási szabványoknak.

4.5. Az XML sémák adott esetben olyan vonatkozó szabványokat vagy szókészleteket használnak, amelyek a séma keretében meghatározott elemek és típusok megfelelő validálásához szükségesek. Ezek a szabványok vagy szókészletek a következőket foglalhatják magukban:

a) az uniós e-igazságügyi alapszókészlet;

b) nem minősített adattípusok;

c) európai uniós nyelvkódlista.

4.6. A biztonsági és hitelesítési protokollok esetében a decentralizált informatikai rendszer szabványokon alapuló protokollokra épül, például:

a) a hálózatokon keresztül történő titkosított és hitelesített kommunikációhoz TLS (Transport Layer Security), a kölcsönös hitelesítés X.509 digitális tanúsítványokon keresztüli támogatásával;

b) a biztonságos hitelesítéshez és engedélyezéshez OAuth/OpenID Connect (OIDC);

c) a biztonságos kulcscseréhez és üzenetintegritás-ellenőrzéshez PKI (nyilvános kulcsú infrastruktúra) és digitális aláírások, megbízható tanúsító hatóságok által kiadott digitális tanúsítványok (X.509) használatával.

5. **Információbiztonsági célkitűzések és a vonatkozó műszaki intézkedések**

5.1. A decentralizált informatikai rendszeren keresztül történő információcsere tekintetében az információtechnológiai biztonsági minimumkövetelmények betartását biztosító műszaki intézkedések az alábbiakat foglalják magukban:

a) az információ bizalmas jellegét biztosító intézkedések, többek között biztonságos kommunikációs csatornák használata;

b) az adatok sértetlenségének biztosítására irányuló intézkedések inaktív állapotban és továbbítás alatt;

c) a decentralizált informatikai rendszeren belül az információküldő eredetének letagadhatatlanságát és az információ beérkezésének letagadhatatlanságát biztosító intézkedések;

d) az információbiztonsági eseményeknek az információtechnológiai biztonsági előírásokra vonatkozó nemzetközi ajánlásokkal összhangban történő naplózását biztosító intézkedések ([1]);

e) a felhasználók hitelesítését és engedélyezését, valamint a decentralizált informatikai rendszerhez kapcsolódó rendszerek azonosságának ellenőrzését lehetővé tévő intézkedések;

5.2. A decentralizált informatikai rendszer komponensei biztosítják a biztonságos kommunikációt és adatátvitelt, ennek érdekében a hitelesítéshez és a biztonságos kulcscseréhez titkosítást és digitális tanúsítványokra épülő nyilvános kulcsú infrastruktúrát, az üzenetek bizalmas jellegének és integritásának fenntartása érdekében pedig biztonságos üzenetküldési protokollokat – AS4 (ebMS), RESTful API-k, SOAP – használnak.

5.3. Amennyiben a TLS-t a decentralizált informatikai rendszerrel összefüggésben alkalmazzák, a protokoll legfrissebb stabil változatát, vagy ennek hiányában ismert biztonsági sebezhetőségeket nem tartalmazó változatot kell használni. Csak olyan kulcshosszok megengedettek, amelyek megfelelő szintű kriptográfiai biztonságot biztosítanak, és nem használhatók olyan titkosítási eszközkészletek, amelyekről ismert, hogy nem biztonságosak, vagy elavultak.

5.4. A decentralizált informatikai rendszer működéséhez használt PKI-tanúsítványokat lehetőség szerint a 910/2014/EU európai parlamenti és tanácsi rendelettel összhangban minősített bizalmi szolgáltatóként elismert tanúsító hatóságok állítják ki ([2]). Intézkedéseket kell végrehajtani annak biztosítása érdekében, hogy az ilyen tanúsítványokat kizárólag rendeltetésüknek megfelelően, a szükséges megbízhatósági szinten és a 910/2014/EU rendelet alkalmazandó követelményeinek megfelelően használják fel.

5.5. A decentralizált informatikai rendszer komponenseit a beépített és alapértelmezett adatvédelem elvével összhangban kell fejleszteni, és megfelelő adminisztratív, szervezeti és technikai intézkedéseket kell végrehajtani a magas szintű kiberbiztonság biztosítása érdekében.

5.6. A Bizottság az (EU) 2018/1725 rendeletben meghatározott adatvédelmi követelményekkel és elvekkel összhangban megtervezi, fejleszti és karbantartja a referenciaimplementációt. A Bizottság által biztosított referenciaimplementáció lehetővé teszi a tagállamok számára az (EU) 2016/679 európai parlamenti és tanácsi rendelet ([3]) és az (EU) 2016/680 irányelv szerinti kötelezettségeik teljesítését.

([1]) A biztonsági célú naplózás sérelme nélkül a decentralizált informatikai rendszer komponensei által alkalmazott naplózási mechanizmusoknak adott esetben lehetővé kell tenniük az (EU) 2018/1725 rendelet 88. cikkében és adott esetben a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/680 európai parlamenti és tanácsi irányelv (HL L 119., 2016.5.4., 89. o., ELI: http://data.europa.eu/eli/dir/2016/680/oj) 25. cikkében meghatározott követelményeknek való megfelelést.

([2]) Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (HL L 257., 2014.8.28., 73. o., ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([3]) Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o., ELI: http://data.europa.eu/eli/reg/2016/679/oj).

5.7. Azok a tagállamok, amelyek a referenciaimplementációtól eltérő nemzeti háttérrendszert használnak, végrehajtják az annak biztosításához szükséges intézkedéseket, hogy a nemzeti háttérrendszer megfeleljen az (EU) 2016/679 rendelet és adott esetben az (EU) 2016/680 irányelv követelményeinek.

5.8. Az Eurojust végrehajtja a szükséges intézkedéseket annak biztosítása érdekében, hogy háttérrendszere vagy az általa alkalmazott referenciaimplementáció-szoftver egy példánya megfeleljen az (EU) 2018/1725 és az (EU) 2018/1727 rendelet követelményeinek.

5.9. A tagállamok és az Eurojust a vonatkozó szakpolitikáikkal összhangban megbízható mechanizmusokat hoznak létre a fenyegetések észlelése és a biztonsági eseményekre való reagálás céljából, amelyekkel biztosítják a biztonsági események időben történő azonosítását, mérséklését és az azokat követő helyreállítást a decentralizált informatikai rendszer részét képező, felelősségi körükbe tartozó informatikai rendszerek tekintetében.

6. **A rendszer által biztosított szolgáltatások hozzáférhetőségével kapcsolatos minimumcélok**

6.1. Az Eurojust és a tagállamok biztosítják, hogy a decentralizált informatikai rendszer felelősségi körükbe tartozó komponensei a hét minden napján 24 órában rendelkezésre álljanak, évente legalább 98 %-os műszaki rendelkezésreállási aránnyal, kivéve a tervezett karbantartást.

6.2. A Bizottság gondoskodik arról, hogy a bírósági adatbázis a hét minden napján 24 órában rendelkezésre álljon, évente 99 %-ot meghaladó műszaki rendelkezésreállási aránnyal, kivéve a tervezett karbantartást.

6.3. Lehetőség szerint munkanapokon a karbantartási műveleteket közép-európai idő szerint 20:00 és 7:00 óra közé kell ütemezni.

6.4. A tagállamok az alábbiak szerint értesítik a Bizottságot, az Eurojustot és a többi tagállamot a karbantartási tevékenységekről:

a) 5 munkanappal korábban olyan karbantartási műveletek esetén, amelyek legfeljebb 4 órás hozzáférhetetlenséget okozhatnak;

b) 10 munkanappal korábban olyan karbantartási műveletek esetén, amelyek 4–12 órás hozzáférhetetlenséget okozhatnak;

c) 30 munkanappal korábban olyan karbantartási műveletek esetén, amelyek több mint 12 órás hozzáférhetetlenséget okozhatnak;

6.5. Amennyiben a tagállamok rögzített rendszeres karbantartási idősávokkal rendelkeznek, tájékoztatják a Bizottságot, az Eurojustot és a többi tagállamot ezen idősávok ütemezett napjáról és időpontjáról. Az első mondatban meghatározott kötelezettségektől eltérően amennyiben a decentralizált informatikai rendszer tagállamok felelősségi körébe tartozó komponensei a rögzített rendszeres karbantartási idősávok valamelyikében nem állnak rendelkezésre, a tagállamok dönthetnek úgy, hogy nem minden alkalommal értesítik a Bizottságot.

6.6. A decentralizált informatikai rendszer tagállamok felelősségi körébe tartozó komponensének váratlan műszaki meghibásodása esetén a tagállamok haladéktalanul tájékoztatják a Bizottságot és a többi tagállamot a hibáról, és amennyiben ismert, az elhárítás tervezett idejéről.

6.7. Az Eurojust az alábbiak szerint értesíti a Bizottságot és a tagállamokat a karbantartási tevékenységekről:

a) 5 munkanappal korábban olyan karbantartási műveletek esetén, amelyek legfeljebb 4 órás hozzáférhetetlenséget okozhatnak;

b) 10 munkanappal korábban olyan karbantartási műveletek esetén, amelyek 4–12 órás hozzáférhetetlenséget okozhatnak;

c) 30 munkanappal korábban olyan karbantartási műveletek esetén, amelyek több mint 12 órás hozzáférhetetlenséget okozhatnak;

6.8. Amennyiben az Eurojust rögzített rendszeres karbantartási idősávokkal rendelkezik, tájékoztatja a Bizottságot és a többi tagállamot ezen idősávok ütemezett napjáról és időpontjáról. Az első mondatban meghatározott kötelezettségektől eltérően amennyiben a decentralizált informatikai rendszer Eurojust felelősségi körébe tartozó komponensei a rögzített rendszeres karbantartási idősávok valamelyikében nem állnak rendelkezésre, az Eurojust dönthet úgy, hogy nem minden alkalommal értesíti a Bizottságot.

6.9. A decentralizált informatikai rendszer Eurojust felelősségi körébe tartozó komponensének váratlan műszaki meghibásodása esetén az Eurojust haladéktalanul tájékoztatja a Bizottságot és a többi tagállamot a hibáról, és amennyiben ismert, az elhárítás tervezett idejéről.

6.10. Az illetékes hatósági/bírósági adatbázis váratlan műszaki meghibásodása esetén a Bizottság haladéktalanul tájékoztatja az Eurojustot és a tagállamokat az elérhetetlenségről, és amennyiben ismert, az elhárítás tervezett idejéről.

6.11. A szolgáltatás zavara esetén a tagállamok és az Eurojust biztosítják a szolgáltatás gyors helyreállítását és a minimális adatvesztést, összhangban a helyreállítási időre és a helyreállítási pontra vonatkozó célkitűzéssel.

6.12. A tagállamok és az Eurojust megfelelő intézkedéseket hajtanak végre a fent vázolt rendelkezésreállási célkitűzések elérésére, és eljárásokat dolgoznak ki a biztonsági eseményekre való hatékony reagálás céljából.

7. **Illetékes hatósági/bírósági adatbázis (CDB)**

7.1. Az (EU) 2018/1727 rendelet 22a. cikke értelmében a decentralizált informatikai rendszer lehetővé teszi az illetékes nemzeti hatóságok és az Eurojust közötti elektronikus kommunikációt. Figyelembe véve az illetékes nemzeti hatóságok és az Eurojust közötti információcserére vonatkozó, a 21., 21a. és 22. cikk szerinti kötelezettségeket, valamint az Eurojust szerepét az (EU) 2018/1727 rendelet 8. cikkének (1) bekezdése szerinti kölcsönös jogsegély vagy kölcsönös elismerés iránti kérelmek kiadásának és végrehajtásának elősegítésében és támogatásában, az érintett illetékes hatóságoknak egyértelműen azonosíthatónak kell lenniük a decentralizált informatikai rendszer használata során. Következésképpen elengedhetetlen az e hatóságok által a decentralizált informatikai rendszer céljából szolgáltatott információk hiteles adatbázisának létrehozása.

7.2. A CDB strukturált formában tartalmazza a következő információkat:

a) az (EU) 2018/1727 rendelet 8. cikke (1) bekezdésének, 8. cikke (3) bekezdésének, 8. cikke (4) bekezdésének, 21., 21a. és 22. cikkének alkalmazásában az illetékes nemzeti hatóságokra, köztük az említett rendelet 20. cikkében meghatározott nemzeti kapcsolattartókra, valamint az említett rendelet 7. cikke ([4]) szerinti nemzeti tagokra vonatkozó információk;

b) adott esetben a hatóságok illetékességi területének vagy hatáskörének meghatározásához szükséges információk, vagy az illetékességük vagy hatáskörük megállapításához szükséges egyéb releváns kritériumok;

c) a decentralizált informatikai rendszeren belüli megfelelő technikai üzenettovábbításhoz szükséges információk.

7.3. A Bizottság felel a CDB fejlesztéséért, karbantartásáért, üzemeltetéséért és támogatásáért.

7.4. A CDB lehetővé teszi a tagállamok és az Eurojust számára az abban szereplő információk frissítését, valamint az illetékes nemzeti hatóságok és a decentralizált informatikai rendszerben részt vevő nemzeti tagok számára ezen információk programozott elérését és lekérdezését;

7.5. A CDB-hez közös kommunikációs protokollon keresztül lehet hozzáférni, függetlenül attól, hogy a decentralizált informatikai rendszerhez csatlakozó illetékes hatóságok működtetnek-e nemzeti háttérrendszert vagy telepített referenciaimplementáció-szoftvert;

7.6. A tagállamok biztosítják, hogy az illetékes hatóságaikra vonatkozóan a CDB adatbázisban szereplő, a 7.2. pontban meghatározott információk teljeskörűek, pontosak és naprakészek legyenek.

([4]) Ez nem érinti a nemzeti tagról a helyettesére, a nemzeti iroda egyéb alkalmazottaira vagy az Eurojust felhatalmazott személyzetére történő hatáskör-átruházást.

II. MELLÉKLET

DIGITÁLIS ELJÁRÁSI SZABVÁNYOK

Az (EU) 2022/850 rendelet 3. cikkének 9. pontjában foglalt meghatározás szerint digitális eljárási szabvány az üzleti folyamatmodellekre és az adatsémákra vonatkozó olyan műszaki előírások összessége, amelyek meghatározzák az e-CODEX-rendszer keretében megosztott adatok elektronikus struktúráját.

Ez a melléklet az üzleti folyamatmodellekre vonatkozó műszaki előírásokat és az adatsémák műszaki előírásait határozza meg.

1. **Az (EU) 2018/1727 rendelet szerinti üzleti folyamatmodellekre vonatkozó műszaki előírások**

Az üzleti folyamatmodellekre vonatkozó műszaki előírásokat az 1.1–1.5. pont tartalmazza. Ezek meghatározzák az (EU) 2018/1727 rendelet alkalmazásában a decentralizált informatikai rendszeren keresztül történő elektronikus kommunikáció lehetővé tételéhez szükséges kulcsfontosságú szempontokat.

A decentralizált informatikai rendszer csak a tagállam illetékes nemzeti hatóságai és az adott tagállam nemzeti tagja közötti információcserét teszi lehetővé.

1.1. *Az (EU) 2018/1727 rendelet 21a. cikke szerinti, az európai terrorizmusellenes igazságügyi nyilvántartással (CTR) kapcsolatos információcsere*

1.1.1. CTR-adattovábbítás modellje:

Az illetékes nemzeti hatóság továbbítja a terrorista bűncselekményekkel kapcsolatos CTR-adatokat a nemzeti tagnak.

1.1.2. CTR-adatfogadás modellje:

A nemzeti tag fogadja a CTR-adatokat.

1.1.3. Hozzájárulási kérelem modellje:

A nemzeti tag az illetékes nemzeti hatósága hozzájárulását kéri.

1.1.4. Hozzájárulási kérelem fogadásának modellje:

Az illetékes nemzeti hatóság fogadja a hozzájárulási kérelmet.

1.1.5. Hozzájárulási kérelemmel kapcsolatos válaszküldés modellje:

Az illetékes nemzeti hatóság választ küld a hozzájárulási kérelemre.

1.1.6. Hozzájárulási kérelemmel kapcsolatos válaszfogadás modellje:

A nemzeti tag fogadja a hozzájárulási kérelemre adott választ.

1.1.7. Kapcsolódási tájékoztatás modellje:

A nemzeti tag tájékoztatja az illetékes nemzeti hatóságot a másik üggyel való kapcsolatról.

1.1.8. CTR-adatfrissítés modellje:

Az illetékes nemzeti hatóság továbbítja a frissítést vagy törlést igénylő adatokat saját nemzeti tagjának.

1.1.9. Az aktualizált CTR-adatok fogadásának modellje:

A nemzeti tag fogadja azokat a CTR-adatokat, amelyek frissítést vagy törlést igényelnek.

1.2. *A súlyos bűncselekményekkel kapcsolatos információcsere – az (EU) 2018/1727 rendelet 21. cikke*

1.2.1. A határokon átnyúló súlyos bűncselekményekkel kapcsolatos adattovábbítás modellje:

Az illetékes nemzeti hatóság továbbítja az Eurojustnak a határokon átnyúló súlyos bűncselekményekre vonatkozó adatokat.

1.2.2. A határokon átnyúló súlyos bűncselekményekkel kapcsolatos adatfogadás modellje:

A nemzeti tag fogadja a határokon átnyúló súlyos bűncselekményekre vonatkozó adatokat.

1.2.3. Hozzájárulási kérelem modellje:

A nemzeti tag az illetékes nemzeti hatósága hozzájárulását kéri.

1.2.4. Hozzájárulási kérelem fogadásának modellje:

Az illetékes nemzeti hatóság fogadja a hozzájárulási kérelmet.

1.2.5. Hozzájárulási kérelemmel kapcsolatos válaszküldés modellje:

Az illetékes nemzeti hatóság választ küld a hozzájárulási kérelemre.

1.2.6. Hozzájárulási kérelemmel kapcsolatos válaszfogadás modellje:

A nemzeti tag fogadja a hozzájárulási kérelemre adott választ.

1.2.7. Kapcsolódási tájékoztatás modellje:

A nemzeti tag tájékoztatja az illetékes nemzeti hatóságot a másik üggyel való kapcsolatról.

1.2.8. A határokon átnyúló súlyos bűncselekményekkel kapcsolatos adatfrissítés modellje:

Az illetékes nemzeti hatóság továbbítja a frissítést vagy törlést igénylő adatokat saját nemzeti tagjának.

1.2.9. A határokon átnyúló súlyos bűncselekményekkel kapcsolatos frissített adatok fogadásának modellje:

A nemzeti tag megkapja a határokon átnyúló súlyos bűncselekményekre vonatkozó, frissítést vagy törlést igénylő adatokat.

1.3. *Általános információk cseréje*

1.3.1. Információküldés modellje:

A nemzeti tag információt küld az illetékes nemzeti hatóságnak, vagy fordítva.

1.3.2. Információfogadás modellje:

Az illetékes nemzeti hatóság vagy a nemzeti tag fogadja az információkat.

1.3.3. Az információval kapcsolatos válaszadás modellje:

Az illetékes nemzeti hatóság válaszol a nemzeti tagtól kapott információkra, vagy fordítva.

1.3.4. Válaszfogadási modell:

A nemzeti tag fogadja a választ az illetékes nemzeti hatóságtól.

1.3.5. Információküldés modellje:

Az illetékes nemzeti hatóság megküldi az információkat a nemzeti tagnak.

1.3.6. Információfogadás modellje:

A nemzeti tag fogadja az információkat.

1.3.7. Az információval kapcsolatos válaszadás modellje:

A nemzeti tag válaszol az illetékes nemzeti hatóságtól kapott információkra.

1.3.8. Válaszfogadási modell:

Az illetékes nemzeti hatóság megkapja a választ a nemzeti tagtól.

1.4. *Könnyítő és támogató szerep – az (EU) 2018/1727 rendelet 8. cikkének (1) bekezdése*

Megjegyzés: Amennyiben az 1.5. pontban ismertetett könnyítési és támogatási modellek a büntetőügyekben folytatott igazságügyi együttműködés területére vonatkozó uniós jogi aktusok által létrehozott, jogszabályban előírt formanyomtatványok cseréjét foglalják magukban, a modelleknek – amennyiben rendelkezésre állnak – az említett jogi aktusokhoz kidolgozott releváns strukturált adatmegjelenítéseket és XML-sémákat kell használniuk, például az (EU) 2023/2844 végrehajtási rendelet vagy más releváns eszközök alkalmazásában létrehozottakat.

1.5. *Könnyítési vagy támogatási kérelem modellje:*

1.5.1. A könnyítési vagy támogatási kérelem továbbításának modellje:

Az illetékes nemzeti hatóság könnyítés iránti kérelmet vagy támogatás iránti kérelmet továbbít saját nemzeti tagjának.

1.5.2. Könnyítési vagy támogatási kérelem fogadásának modellje:

A nemzeti tag fogadja a könnyítési vagy támogatási kérelmet, és azt a JUDEX-en kívül továbbítja a megkeresett tagállam nemzeti tagjának.

1.5.3. Könnyítési vagy támogatási kérelem illetékes nemzeti hatósághoz való továbbításának modellje:

A megkeresett tagállam nemzeti tagja megküldi a megkeresést saját illetékes nemzeti hatóságának.

1.5.4. Könnyítési vagy támogatási kérelem fogadásának modellje:

Az illetékes nemzeti hatóság fogadja a könnyítési vagy támogatási kérelmet.

1.5.5. A könnyítési vagy támogatási kérelemmel kapcsolatos válaszküldés modellje:

Az illetékes nemzeti hatóság választ vagy információt küld a megkeresett tagállam nemzeti tagjának a megkeresésre.

1.5.6. A könnyítési vagy támogatási kérelemmel kapcsolatos válaszfogadás modellje:

A nemzeti tag fogadja az illetékes nemzeti hatóságtól a segítségnyújtási vagy támogatási kérelemre adott választ vagy az arra vonatkozó információkat, és a JUDEX-en kívül megosztja azt a megkereső tagállam nemzeti tagjával.

1.5.7. A könnyítési vagy támogatási kérelemmel kapcsolatos válaszadás modellje:

A megkereső tagállam nemzeti tagja válaszol vagy megosztja az illetékes nemzeti hatóságtól származó, a könnyítési vagy támogatási kérelemre vonatkozó információkat.

1.5.8. Válaszfogadási modell:

Az illetékes nemzeti hatóság fogadja a könnyítési vagy támogatási kérelemre adott választ vagy az arra vonatkozó információkat.

2. **Az adatsémákra vonatkozó műszaki előírások**

Az (EU) 2018/1727 rendelet digitalizálásához szükséges XML-sémaleírások kidolgozásának alapjául szolgáló műszaki előírásokat e melléklet 2.1. és 2.2. pontja tartalmazza. Ezek az előírások meghatározzák a fő komponenseket és az egyéb információtat annak érdekében, hogy átfogó leírást nyújtsanak e sémák előállításához.

A leírás célja, hogy általános jellegénél fogva lehetővé tegye az előállított XSD-k módosítását és kiterjesztését anélkül, hogy ezen előírások jelentős módosítására lenne szükség.

Az előírások a sémáknak az (EU) 2018/1727 rendelethez csatolt, jogszabályban előírt formájára, az előre meghatározott üzenetekre vagy az említett rendelet szerinti információcserék során használt szabad szöveges üzenetekre vonatkoznak.

2.1. *Általános szempontok*

Valamennyi rendelkezésre bocsátandó sémára a következő rendelkezéseket kell alkalmazni:

2.1.1. Verziókezelés

Verzióattribútumot kell feltüntetni, amely megkönnyíti a sémaverziók kezelését, és lehetővé teszi a rendszer jövőbeli iterációk során történő frissítését az üzleti követelményeknek megfelelően. Új funkciók vagy finomítások bevezetésekor a verzióattribútumnak jeleznie kell, hogy az új verzió visszafelé kompatibilis-e.

2.1.2. Sémadeklaráció és metaadatok

— A séma adott esetben olyan vonatkozó – az e-CODEX által az interoperabilitáshoz megkövetelt – szabványokat vagy szókészleteket használ, amelyek a séma keretében meghatározott elemek és típusok megfelelő validálásához szükségesek. Ezek az alábbiak lehetnek:

  — az uniós e-igazságügyi alapszókészlet,

  — nem minősített adattípusok,

  — európai uniós nyelvkódlista.

— Emellett adott esetben a séma tartalmazhatja a vonatkozó ETSI-szabványokat azok definícióinak alkalmazása érdekében.

2.1.3. Annotációk és dokumentáció

— **Magyarázó jegyzetek**: A séma minden elemét jellemzően magyarázó jegyzeteknek kell kísérniük. A magyarázó jegyzetek ember által olvasható információkat nyújtanak az elemről, sok esetben annak célját vagy használatát határozzák meg egyértelműen és tömören.

2.1.4. Használat és adaptálhatóság

A sémának az a)–d) pontban meghatározott szabályokat kell követnie:

a) **Moduláris szerkezet**: az egyes szakaszokat meghatározott funkciókkal kell megtervezni, úgy, hogy külön-külön újrahasználhatók vagy kiigazíthatók legyenek. Ez megkönnyíti a sémának a különböző felhasználási eseteknek megfelelő testre szabását.

b) **Kiterjeszthetőség**: a sémát úgy kell kialakítani, hogy támogassa új elemek vagy attribútumok felvételét, amennyiben a jövőben további információkra lesz szükség. Ezt opcionális elemek és sorrendek alkalmazásával kell elérni, amelyek a meglévő végrehajtás megszakítása nélkül meghosszabbíthatók.

c) **Adaptálható struktúra**: a séma kialakításának lehetővé kell tennie elemek vagy adattípusok szükség szerinti hozzáadását vagy módosítását. A sémának a követelmények változásait figyelembe kell vennie anélkül, hogy nagyobb átalakításra lenne szükség.

d) **Opcionális elemek**: a sémán belüli elemek választhatóként jelölhetők meg, azaz meghatározott körülmények alapján beilleszthetők vagy elhagyhatók.

A sémát úgy kell kialakítani, hogy támogassa a strukturált adatok gyűjtését konkrét kérésekhez.

2.1.5. Módosítások

A sémát rugalmasságnak, modularitásnak és könnyű alkalmazkodásnak kell jellemeznie. Az összetett típusokat és választható elemeket úgy kell beépíteni a kialakításba, hogy azok különböző forgatókönyveket kezelhessenek, ugyanakkor könnyen módosíthatók és kiterjeszthetők maradjanak.

2.2. *Strukturált adatok cseréje*

A 2.2.1. és 2.2.2. pontban említett strukturált adatokat az (EU) 2018/1727 rendelet 22a. cikkének (3) bekezdésével összhangban kell átadni. A sémának lehetővé kell tennie azon adatkészletek feltüntetését is, amelyeket a későbbi frissítésekből törölni kell.

2.2.1. Az európai terrorizmusellenes igazságügyi nyilvántartás adatai

Az adatsémára vonatkozó alábbi műszaki előírások strukturált keretet hoznak létre a séma XML-formátumú létrehozásához.

a) Felső szintű szakasz

Ez a felső szintű szakasz megfelel az (EU) 2018/1727 rendelet III. mellékletében meghatározott, az európai terrorizmusellenes igazságügyi nyilvántartás (CTR) számára átadott információknak.

b) Az üzenet felépítése

A CTR-adatok struktúrája elemek sorozatából áll, és legalább a következőket tartalmazza:

i. természetes személyek azonosítására szolgáló információk:

— vezetéknév (családi név),

— utónevek (keresztnevek),

— bármilyen álnév,

— születési idő,

— születési hely (város és ország),

— állampolgárság vagy állampolgárságok,

— személyazonossági okmány (az okmány típusa és száma),

— nem,

— lakóhely;

ii. jogi személyek azonosítására szolgáló információk:

— a vállalkozás neve,

— társasági forma,

— a központi ügyvezetés helye;

iii. természetes és jogi személyek azonosítására szolgáló információk:

— telefonszámok,

— e-mail-címek,

— bankoknál vagy más pénzügyi intézményeknél vezetett bankszámlák részletes adatai,

— jogállás az eljárásban;

iv. a bűncselekménnyel kapcsolatos információk:

— terrorista bűncselekmény előkészítésében vagy elkövetésében részt vevő jogi személyekre vonatkozó információk,

— a bűncselekmény jogi minősítése a nemzeti jog szerint,

— az I. mellékletben található felsorolásban szereplő súlyos bűncselekmény,

— terrorista csoporttal való bármely kapcsolat,

— a terrorizmus típusa, például dzsihádista, szeparatista, baloldali vagy jobboldali,

— az ügy rövid összefoglalása;

v. tájékoztatás a nemzeti eljárásról:

— az ilyen eljárás állása,

— felelős ügyészség,

— ügyszám,

— a hivatalos bírósági eljárás megindításának időpontja,

— más jelentős ügyekkel fennálló kapcsolat;

vi. kiegészítő információk mező (szabad szöveg);

vii. előzetes engedélyezési kód.

2.2.2. Az (EU) 2018/1727 rendelet 21. cikkének megfelelő adatátvitel.

a) Az (EU) 2018/1727 rendelet 21. cikkének (4) bekezdése, közös nyomozócsoportok létrehozása

i. Felső szintű szakasz

Ez a felső szintű szakasz megfelel az (EU) 2018/1727 rendelet 21. cikkének (4) bekezdésében meghatározott, a közös nyomozócsoportok létrehozására vonatkozó információknak.

ii. Az üzenet struktúrája

Az adatok struktúrája elemek sorozatából áll, és legalább a következőket tartalmazza:

— A büntetőeljárásért felelős nemzeti igazságügyi hatóság

— A büntetőeljárás nemzeti hivatkozási száma

— A büntetőeljárás állása

— Kivizsgált bűncselekmények

— Az ügyben érintett egyéb országok

— Az Eurojust által már támogatott ügy?

— Ha igen, Eurojust-ügyazonosító

— Ha nem, akkor ez támogatási kérelem?

— Az Europol által támogatott ügy?

— Ha igen, az operatív munkacsoport (OTF) és/vagy a Biztonságos Információcsere Hálózati Alkalmazás (SIENA)?

— A közös nyomozócsoportra vonatkozó megállapodás:

— Részt vevő országok

— A közös nyomozócsoport részes felei (a vizsgálatokért felelős nemzeti hatóságok)

— A közös nyomozócsoport hatálya alá tartozó büntetőeljárások nemzeti hivatkozási száma

— Aláírás dátuma

— Időtartam

— Kivizsgált bűncselekmények

— Az ügy rövid összefoglalása

— A közös nyomozócsoporthoz tartozó büntetőeljárás fő gyanúsítottjai (vezetéknév, utónév, születési idő és hely, valamint adott esetben a II. melléklet szerinti egyéb releváns és szükséges adatkategóriák)

— A közös nyomozócsoportok munkájának eredményei:

— Az alábbiakat érintő nehézségek/késések:

— a közös nyomozócsoport létrehozása,

— bizonyítékok bekérése/megosztása a közös nyomozócsoporton belül,

— közös büntetőeljárási stratégia elfogadása/végrehajtása,

— A közös nyomozócsoport bizonyítékainak elfogadhatósága/elfogadhatatlansága/értékelése a nemzeti eljárásokban,

— A bírósági eljárás eredménye (sikeres/sikertelen büntetőeljárások és büntetőítéletek/felmentő ítéletek)

iii. Előzetes engedélyezési kód

b) Az (EU) 2018/1727 rendelet 21. cikkének (5) bekezdése, súlyos, összetett esetek

i. Felső szintű szakasz

Ez a felső szintű szakasz megfelel az Eurojust-rendelet 21. cikkének (5) bekezdésében meghatározott információknak, azaz a súlyos, összetett ügyeknek.

ii. Az üzenet struktúrája

Az adatok struktúrája elemek sorozatából áll, és legalább a következőket tartalmazza:

— A büntetőeljárásért felelős nemzeti igazságügyi hatóság

— A büntetőeljárás nemzeti hivatkozási száma

— A büntetőeljárás állása

— Kivizsgált bűncselekmények

— Az ügyben érintett egyéb országok

— Az Eurojust által már támogatott ügy?

— Ha igen, Eurojust-ügyazonosító

— Ha nem, akkor ez támogatási kérelem?

— Az Europol által támogatott ügy?

— Ha igen, az operatív munkacsoport és/vagy SIENA?

— A súlyos bűncselekmény alkalmazandó formája

— Szervezett bűnözői hálózat érintettsége

— Maffiatípusú

— Transznacionális szervezett bűnözői hálózat

— Uniós szintű következmények

— A büntetőeljárás fő gyanúsítottjai (vezetéknév, utónév, születési idő és hely, valamint adott esetben a II. melléklet szerinti egyéb releváns és szükséges adatkategóriák)

— Az ügy rövid összefoglalása

— Egyéb érintett országok

— Országok, amelyekkel már megkezdődött az együttműködés

— Más országban érintett illetékes hatóságok

— Alkalmazott igazságügyi együttműködési eszközök

— A küldött/beérkezett megkeresések száma

— Kapcsolódó vizsgálatok megléte

— Azon országok, amelyekkel az együttműködést aktiválni kell/lehetőleg érintett országok

— A szükséges együttműködés típusa (például kiadatás, bizonyítékgyűjtés, egyéb együttműködés)

— Kapcsolódó vizsgálatok megléte

iii. Előzetes engedélyezési kód

c) Az (EU) 2018/1727 rendelet 21. cikke (6) bekezdésének a) pontja, joghatósági összeütközések

i. Felső szintű szakasz

Ez a felső szintű szakasz megfelel az (EU) 2018/1727 rendelet 21. cikke (6) bekezdésének a) pontjában meghatározott információknak, azaz a joghatósági összeütközéseknek.

ii. Az üzenet struktúrája

Az adatok struktúrája elemek sorozatából áll, és legalább a következőket tartalmazza:

— A büntetőeljárásért felelős nemzeti igazságügyi hatóság

— A büntetőeljárás nemzeti hivatkozási száma

— A büntetőeljárás állása (pl. nyomozás, büntetőeljárás, tárgyalás)

— Kivizsgált bűncselekmények

— Az ügyben érintett egyéb országok

— Az Eurojust által már támogatott ügy?

— Ha igen, Eurojust-ügyazonosító

— Ha nem, akkor ez támogatási kérelem?

— Az Europol által támogatott ügy?

— Ha igen, az operatív munkacsoport és/vagy SIENA?

— Egyéb érintett országok

— A másik ország illetékes nemzeti hatóságai, ha ismertek

— A más országban folytatott büntetőeljárások nemzeti hivatkozási száma

— Az eljárás szakasza egy másik országban, ha ismert

— Pozitív vagy negatív összeütközés

— Tényleges vagy potenciális összeütközés

— Már megkezdett koordinációs tevékenységek (pl. a 2009/948/IB tanácsi kerethatározat ([1]) szerinti konzultációk)

— Az ügy rövid összefoglalása

— A fő közös gyanúsítottak (vezetéknév, utónév, születési idő és hely, valamint adott esetben a II. melléklet szerinti egyéb releváns és szükséges adatkategóriák)

iii. Előzetes engedélyezési kód

d) 21. cikk, (6) bekezdés, b) pont, ellenőrzött szállítások

i. Felső szintű szakasz

Ez a felső szintű szakasz megfelel az (EU) 2018/1727 rendelet 21. cikke (6) bekezdésének b) pontjában meghatározott információknak: ellenőrzött szállítások

ii. Az üzenet struktúrája

Az adatok struktúrája elemek sorozatából áll, és legalább a következőket tartalmazza:

— A büntetőeljárásért felelős nemzeti igazságügyi hatóság

— A büntetőeljárás nemzeti hivatkozási száma

— A büntetőeljárás állása (pl. nyomozás, büntetőeljárás, tárgyalás)

— Kivizsgált bűncselekmények

— Az ügyben érintett egyéb országok

— Az Eurojust által már támogatott ügy?

— Ha igen, Eurojust-ügyazonosító

— Ha nem, akkor ez támogatási kérelem?

— Az Europol által támogatott ügy?

— Ha igen, az operatív munkacsoport és/vagy SIENA?

— Egyéb érintett országok

— Származási, átutazási vagy célország

— Más országok illetékes nemzeti hatóságai

— Kapcsolódó vizsgálatok megléte más országokban

([1]) A Tanács 2009/948/IB kerethatározata (2009. november 30.) a joghatóság gyakorlásával kapcsolatos, büntetőeljárások során felmerülő összeütközések megelőzéséről és rendezéséről (HL L 328., 2009.12.15., 42. o., ELI: http://data.europa.eu/eli/dec_framw/2009/948/oj).

— A szállított áruk típusa (pl. kábítószer, típussal együtt/pénz/fegyver/cigaretta/egyéb)

— Az ellenőrzött szállítás állása (pl. tervezett, folyamatban lévő, befejezett)

— Az ellenőrzött szállítás eredménye, ha már végrehajtották

— Alkalmazott igazságügyi együttműködési eszköz

— A fő közös gyanúsítottak (vezetéknév, utónév, születési idő és hely, valamint adott esetben a II. melléklet szerinti egyéb releváns és szükséges adatkategóriák)

iii. Előzetes engedélyezési kód

e) Az (EU) 2018/1727 rendelet 21. cikke (6) bekezdésének c) pontja, az igazságügyi együttműködési eszközökkel kapcsolatos ismétlődő kérdések

i. Felső szintű szakasz

Ez a felső szintű szakasz megfelel az (EU) 2018/1727 rendelet 21. cikke (6) bekezdésének c) pontjában meghatározott információknak: az igazságügyi együttműködési eszközökkel kapcsolatos ismétlődő problémák.

ii. Az üzenet struktúrája

Az adatok struktúrája elemek sorozatából áll, és legalább a következőket tartalmazza:

— A büntetőeljárásért felelős nemzeti igazságügyi hatóság

— A büntetőeljárás nemzeti hivatkozási száma

— A büntetőeljárás állása (pl. nyomozás, büntetőeljárás, tárgyalás)

— Kivizsgált bűncselekmények

— Az ügyben érintett egyéb országok

— Az Eurojust által már támogatott ügy?

— Ha igen, Eurojust-ügyazonosító

— Ha nem, akkor ez támogatási kérelem?

— Az Europol által támogatott ügy?

— Ha igen, az operatív munkacsoport és/vagy SIENA?

— Egyéb érintett országok

— Illetékes nemzeti hatóságok, ha ismertek

— Kibocsátó vagy végrehajtó hatóságként eljárva

— Érintett igazságügyi együttműködési eszköz (pl. EEP, ENYH, befagyasztás és elkobzás)

— Konkrét megkeresés (azaz milyen nyomozási cselekmény, milyen típusú befagyasztás, a büntetés végrehajtása vagy büntetőeljárás lefolytatása céljából kibocsátott EEP)

— Elutasítás vagy ismételt nehézség

— Elutasítás esetén milyen konkrét indokra hivatkoztak?

— A kérdéskör rövid leírása

— Az ugyanazon probléma által érintett egyéb nemzeti hatóságok, ha vannak ilyenek

iii. Előzetes engedélyezési kód

2.3. *Előzetes engedélyezési kódok*

Az Eurojusttal a JUDEX-en keresztül történő adatmegosztás során az illetékes nemzeti hatóságok előzetes engedélyezési kódokkal jelzik az adatok további kezelését, az azokhoz való hozzáférést és az adattovábbítást a kapcsolat azonosítását követően. Az előzetes engedélyezési kódokban fel kell tüntetni, hogy a kapcsolódásra vonatkozó információk megoszthatók-e más illetékes nemzeti hatóságokkal, más uniós ügynökségekkel és szervekkel, harmadik országokkal vagy nemzetközi szervezetekkel, és ha igen, milyen mértékben.

2.4. *Előre meghatározott üzenetek*

Az előre meghatározott üzenetek az (EU) 2018/1727 rendelettel létrehozott információcsere-nyilatkozatok, amelyekre vonatkozóan a jogi aktus nem tartalmazott konkrét formanyomtatványt. Típusukat és számukat az üzleti és technikai elemzés során határozzák meg.

Az előre meghatározott üzenetekre vonatkozó XLM sémafogalommeghatározásokat (XSD) úgy kell kialakítani, hogy biztosítsák a konzisztenciát, a struktúrát és az üzleti igényeknek való megfelelést.

Ezekre a sémákra a következőket kell alkalmazni:

a) ebben a sémában a felső szintű szakaszt a meghatározott üzenettípus szerint kell megnevezni;

b) az adott üzenettípushoz szükséges mezőket ebben a struktúrában kell megadni és meghatározni, biztosítva az adatelem megfelelő megjelenítését.

2.5. *Szabad szöveges üzenetek*

A szabad szöveges üzenetek olyan üzenetváltások, amelyek strukturálatlan vagy részben strukturált tartalmakat tesznek lehetővé, így rugalmasságot biztosítanak, miközben továbbra is megfelelnek a szabályozási és üzleti követelményeknek. A szabad szöveges üzenetek XSD-jét úgy kell kialakítani, hogy biztosítsa a következetességet és a megfelelő formázást.

Ezekre a sémákra a következőket kell alkalmazni.

a) a sémában a felső szintű szakaszt a meghatározott szabad szöveges üzenettípus szerint kell megnevezni;

b) a sémának meg kell határoznia a szabad szöveges üzenethez szükséges szerkezetet, ugyanakkor lehetővé kell tennie az elemek szükség szerinti megfelelő sorrendjét;

c) az adott szabad szöveges üzenettípushoz szükséges mezőket ebben a struktúrában kell megadni és meghatározni, biztosítva az adatelem megfelelő megjelenítését.

III. MELLÉKLET

AZ UJJNYOMATOKRA ÉS FÉNYKÉPEKRE VONATKOZÓ MŰSZAKI ELŐÍRÁSOK

A decentralizált informatikai rendszeren keresztül váltott üzenetekhez csatolhatók csatolmányok, többek között a Nemzeti Szabványügyi és Technológiai Intézet (NIST) ujjnyomatokat és fényképeket tartalmazó fájljai, az 1. és 2. pontban meghatározott műszaki előírásoknak megfelelően.

1. **Ujjnyomatok**

Azoknak az ujjnyomatoknak, amelyeket a terrorista bűncselekményekkel kapcsolatos büntetőeljárás alá vont személyek megbízható azonosítása céljából meg lehet osztani az Eurojusttal, a következő feltételeknek kell megfelelniük:

a) az ujjnyomatokat egy digitális ujjnyomatképeket tartalmazó fájlban (a továbbiakban: NIST ujjnyomatfájl) adják meg, és az ANSI/NIST-ITL 1–2011. évi, 2015-ben aktualizált szabványnak (vagy újabb verziónak) megfelelően nyújtják be;

b) a NIST ujjnyomatfájl legfeljebb tíz egyéni ujjnyomatból áll: átforgatott, sík vagy mindkettő;

c) minden ujjnyomat címkével rendelkezik;

d) az ujjnyomatokat élő szkenneléssel vagy papírra behelyezve rögzítik, feltéve, hogy a papíron beoltott ujjnyomatokat az előírt felbontásban és azonos minőségben szkennelték;

e) a NIST ujjnyomatfájl lehetővé teszi olyan kiegészítő információk felvételét, mint az ujjnyomat-nyilvántartás feltételei és az egyedi ujjnyomatképek megszerzésének módja.

f) az ujjnyomatok névleges felbontása 500 vagy 1 000 ppi ([1]) (+/– 10 ppi elfogadható eltéréssel), 256 szürkeségi árnyalattal;

g) az ujjnyomatok kompressziós algoritmusa követi a Nemzeti Szabványügyi és Technológiai Intézet (NIST) ajánlásait. Az 500 ppi felbontású ujjnyomatadatokat a WSQ algoritmussal (ISO/IEC 19794–5:2005) tömörítik. Az 1 000 ppi felbontású ujjnyomatadatokat a JPEG 2000 képösszenyomási szabvány (ISO/IEC 15444–1) és kódrendszer alkalmazásával tömörítik. A tömörítés során elérendő arány: 15:1.

2. **Fényképek**

Azoknak a fényképeknek, amelyeket a terrorista bűncselekményekkel kapcsolatos büntetőeljárás alá vont személyek megbízható azonosítása céljából meg lehet osztani az Eurojusttal, a következő feltételeknek kell megfelelniük:

a) a fényképfájlban (NIST fényképfájlban) csak egy arcképmás szerepel, és azt az ANSI/NIST-ITL 1–2011. évi, 2015-ben aktualizált szabványnak (vagy újabb verziónak) megfelelően kell benyújtani;

b) a fényképek szürkeárnyalatos, színes vagy közel infravörös képek;

c) a fényképek minősége az ISO/IEC 19794–5:2011 számú szabvány „szemből készített kép” típusa vagy bármely újabb rendelkezésre álló változat képére vonatkozó követelményeken alapul;

d) a NIST fényképfájl lehetővé teszi kiegészítő információk feltüntetését, beleértve a képfelvétel időpontját is;

([1]) Pixel/hüvelyk.

e) az álló tájolású fényképek felbontása legalább 600 × 800, legfeljebb 1 200 × 1 600 pixel;

f) az arc a fényképen belül úgy helyezkedik el, hogy a szemek középpontja között legalább 120 pixelnyi távolság legyen;

g) a fényképekhez használt kompressziós algoritmus követi a Nemzeti Szabványügyi és Technológiai Intézet (NIST) ajánlásait. A fényképeket csak egyszer tömörítik a JPG (ISO/IEC 10918) vagy JPEG 2000 (ISO/IEC 15444) képtömörítési szabvány és kódrendszer szerint, legfeljebb 20:1 tömörítési arányban.